USING THE SOFTWARE CAPABILITY MATURITY MODEL FOR CERTIFICATION PROJECTS (1998)

Leanna K. Rierson, Federal Aviation Administration, Washington, D.C.

Abstract

The purpose of this paper is to explore the use of the Software Engineering Institute's Software Capability Maturity Model (SW-CMM) on civil aviation projects. The paper will examine SW-CMM and RTCA DO-178B/EUROCAE ED-12B by considering the basic concepts of each standard, keys to successful integration of the standards, and benefits of integrating the two standards.

Introduction

Throughout the 1990s the Software Capability Maturity Model (SW-CMM) has emerged as a yardstick for measuring software process maturity. The SW-CMM was developed at Carnegie Mellon by the Software Engineering Institute. It soon became clear that software process maturity was insufficient without looking further into the systems engineering process and the acquisition life cycle. This led to the development of the Systems Engineering Capability Maturity Model (SE-CMM) and the Systems Acquisition Capability Maturity Model (SA-CMM). The SW-CMM, SE-CMM, and SA-CMM form the foundation for a number of other Capability Maturity Models (CMMs) being developed to meet the specialized needs of the industry. For example, the Federal Aviation Administration's (FAA) Research and Acquisition Organization recently released the Integrated Capability Maturity Model (known as FAA-iCMM) to meet the software, systems, and acquisition needs of the FAA for acquiring software intensive systems. Likewise, a Security Systems CMM was developed for the specialized needs of developing secure systems.

The SW-CMM is based on good, common-sense software engineering practices and provides a measuring process for companies to baseline and improve their processes. These quality attributes give incentive for many avionics developers to implement the SW-CMM into their organizations today. Additionally, many acquirers of avionics systems now require vendors to meet specific SW-CMM levels prior to contract award.

Avionics projects for civil aviation must meet the regulations of the FAA to receive certification or authorization. For the software aspects of certification, the FAA's Advisory Circular 20-115B recognizes RTCA DO-178B, "Software Considerations in Airborne Systems and Equipment Certification", as an acceptable means of compliance for the evaluation of software in airborne systems. The European Community recognizes European Organization for Civil Aviation Equipment (EUROCAE) document ED-12B, which is identical to DO-178B. DO-178B/ED-12B contains a set of objectives that are based on the level of safety required by the system.

As described above, many developers of avionics systems must meet both the SW-CMM and DO-178B/ED-12B. This has led to many questions and concerns regarding the relationship of these two assurance standards. This paper will address the three most often asked questions:

- Are DO-178B/ED-12B and SW-CMM compatible?
- Can SW-CMM be used instead of DO-178B/ED-12B?

- How can a company apply both SW-CMM and DO-178B/ED-12B?

To effectively integrate these two standards for civil certification projects, this paper first provides an overview of both SW-CMM and DO-178B/ED-12B. Next, the paper compares SW-CMM and DO-178B/ED-12B and provides suggestions for integration of the two standards. The paper ends with a summary of the benefits of using SW-CMM on certification projects.

It should be noted that this paper is not the official FAA position. The author is a FAA employee and the paper is intended to be consistent with FAA policy; however, it has not been coordinated through the FAA's approving officials and merely represents the opinions of the author.

Overview of SW-CMM

The SW-CMM framework was started in 1986 by Software Engineering Institute (SEI) with assistance from MITRE Corporation. In 1991, version 1.0 was released and began to be used by the software community. Version 1.0 was revised by the software community in 1991 and 1992—leading to the release of SW-CMM version 1.1 in early 1993. Version 1.1 is currently being used world-wide. SW-CMM provides a model that leads to software process improvement (Paulk, viii).

The SW-CMM categorizes the overall company process maturity into five levels of maturity. For the purpose of SW-CMM, a "software process can be defined as a set of activities, methods, practices, and transformations that people use to develop and maintain software and associated products (e.g., project plans, design documents, code, test cases, and user manuals)" (Paulk, 3). The maturity levels, 1 to 5, indicate the overall effectiveness of the company's software engineering practices (Pressman, 27). Each increasing level is based on achieving the attributes of the previous low levels. The five levels are describe as follows (Paulk, 8-9):

- **Level 1: Initial** – The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort.
- **Level 2: Repeatable** – The project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on project with similar applications.
- **Level 3: Defined** – The software processes for both management and engineering activities is documented, standardized, and integrated into a standard software process for organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.
- **Level 4: Managed** – Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.
- **Level 5: Optimizing** – Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

Each maturity level has associated key process areas (KPAs) that describe the software engineering attributes that must be present to satisfy that particular level (see Table 1). As the maturity level increases, quality and productivity increase and risk of unsuccessful and unpredictable projects decreases. Within each KPA there are goals/objectives that must be achieved to satisfy the KPA. Each KPA is rated using the components described below:

- **Activities** – Tasks to be completed to successfully achieve the KPA.
- **Commitments** – Organizational requirements imposed to assure the activities are carried out.
- **Abilities** – Things in place to enable organization to meet commitments.
- **Measurement of Implementation** – Process of monitoring activities.

- **Verification of Implementation** – Process of assuring that the KPA is being properly achieved.

Table 1. Key Process Areas For SW-CMM

Maturity Levels	Key Process Areas
5 – Optimizing (focus on continuous improvement)	• Process Change Management • Technology Innovation • Defect Prevention
4 – Managed (focus on product & process quality)	• Quality Management • Process Measurement & Analysis
3 – Defined (focus on engineering process)	• Peer Reviews • Intergroup Coordination • Software Product Engineering • Integrated Software Management • Training Program • Organization Process Definition • Organization Process Focus
2 – Repeatable (focus on project management)	• Software Configuration Management • Software Quality Assurance • Software Sub-contract Management • Software Project Tracking & Oversight • Software Project Planning • Software Requirements Management
1 – Initial (focus on individual)	• None

Each KPA is defined by a set of key practices (such as policies, procedures, and activities) that must be in place before the KPA is achieved.

This section has provided a very high overview of the SW-CMM process. There are numerous sources to assist in deeper study of the subject, including the SW-CMM document and the SEI web-site (http://www.sei.cmu.edu).

Overview of DO-178B/ED-12B

DO-178/ED-12 was first developed by the international civil aviation community in 1982. It was revised in 1985 to add more detail. In 1992, DO-178B/ED-12B was completed and has become the software "standard" for airborne software in civil aviation products. The DO-178/ED-12 document and all of its revisions were sponsored by RTCA and EUROCAE, with the involvement of aviation, software, and certification experts from across the world.

DO-178B/ED-12B focuses on the software aspects of system development. As part of the systems engineering task, a system safety assessment must be performed before DO-178B/ED-12B can be applied to the software development effort. A system safety assessment is a process to identify the hazards, failure conditions leading to these hazards, and the effects of mitigation strategies. The safety assessment task determines a software level based upon the contribution of the software to the potential failure conditions defined in the system safety assessment process. The five software levels, A to E, are summarized in Table 2 (DO-178B, page 7).

These software levels define differing degrees of rigor. Annex A in DO-178B/ED-12B lists the objectives that must be met for each specific software level. These software levels define a number of desirable attributes for the software development and verification processes. The differences in rigor are determined by the number of objectives which need to be satisfied, whether a specific objective is satisfied with independence, and the formality of configuration control of the software data produced during development. For example, the number of objectives for each software level is listed below:

- Level A: 66 objectives
- Level B: 65 objectives
- Level C: 58 objectives
- Level D: 28 objectives
- Level E: 0 objectives

DO-178B/ED-12B is divided into development activities and integral processes. The development activities include planning, requirements, design, code, and integration. The integral processes include verification, configuration management, quality assurance, and certification liaison. The integral processes are overlaid on each of the development activities (i.e., verification, configuration management, quality assurance, and certification liaison are applied to each development activity).

Table 2. DO-178B/ED-12B Software Levels

Failure Condition Category	Description	SW Level
Catastrophic	Failure conditions which would prevent continued safe flight and landing of the aircraft.	A
Hazardous	Failure condition which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operation conditions to the extent that there would be: (1) a large reduction in safety margins or functional capabilities, (2) physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely, or (3) adverse effects on occupants including serious or potential fatal injuries to a small number of occupants.	B
Major	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operation conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, as significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries.	C
Minor	Failure conditions which would not significantly reduce aircraft safety, and which would involve crew actions that are well within their capabilities.	D
No Effect	Failure conditions which do not affect the operational capability of the aircraft or increase crew workload.	E

The objectives of DO-178B/ED-12B are listed in Annex A and are organized around the development activities and integral processes previously described. There are ten tables in Annex A with objectives—the subject of each table is listed below:

- Table A-1: Software Planning Process
- Table A-2: Software Development Processes
- Table A-3: Verification of Outputs of Software Requirements Process
- Table A-4: Verification of Outputs of Software Design Process
- Table A-5: Verification of Outputs of Software Coding & Integration Processes
- Table A-6: Testing of Outputs of Integration Process
- Table A-7: Verification of Verification Process Results
- Table A-8: Software Configuration Management Process
- Table A-9: Software Quality Assurance Process
- Table A-10: Certification Liaison Process

Table A-4 objective 1 is used in Figure 1 to illustrate the Annex A table layout and structure. The first set of columns contains information about the DO-178B/ED-12B **objectives**: objective number, description, and reference to DO-178B/ED-12B paragraph where that objective is further detailed. The next set of columns with headers A, B, C, D show the applicability of that particular objective to the software level. For example, objective 1 is applicable for levels A, B, and C; however, it does not need to be satisfied for software level D. If the circle indicating applicability is filled in, then that objective must be satisfied with independence. The next series of columns describe the **outputs** produced as evidence that the objective is satisfied. The "Description" column lists where that data is found. The "Ref." Column identifies the paragraph within Chapter 11 of DO-178B/ED-12B that details the attributes of that software data. The last 4 columns correlate the rigor of configuration management of the particular output with the associated software level. Control category 1 requires more configuration management activities than control category 2. For instance, control category 1 requires problem reporting and change control, where as control category 2 requires only change control.

Assessment to DO-178B/ED-12B is performed through on-site reviews and/or desk-top (data) reviews by FAA personnel, Designated Engineering Representatives, and/or software developer's team members. The assessment evaluates the data to determine if the objectives listed in Annex A of DO-178B/ED-12B are met. In June of 1998, the FAA released a job aid entitled, "Conducting Software Review Prior to Certification". The job aid outlines a process for assuring compliance to the objectives of DO-178B/ED-

12B. The job aid is available electronically and is designed to be tailored to meet the specific needs of the evaluator or project.

Figure 1. Portion of Table A-4 in DO-178B

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Low-level requirements comply with high-level requirements.	6.3.2a	I	I	m		Software Verification Results	11.14	2	2	2	

This section has provided a very high level overview of DO-178B/ED-12B. More information may be obtained by reading DO-178B/ED-12B itself, by participating in related RTCA and EUROCAE activities, and by reviewing the FAA job aid.

Comparison of SW-CMM and DO-178B/ED-12B

Although both SW-CMM and DO-178B/ED-12B are assurance standards, their primary focus is somewhat different. The SW-CMM looks not only at the development processes but also at their management and refinement. The better defined, managed, and improved a process is, the better the software quality and the greater the likelihood that the development is within cost and schedule.

The focus of DO-178B/ED-12B is solely on design assurance. Specific DO-178B/ED-12B objectives are identified to provide the required assurance by criticality level. For level A and B, specific classes of software development errors are targeted for removal from code through stringent verification activities. Although management, cost, and schedule considerations may be important to developers, this is not the purview of FAA certification authorities. FAA authorities are concerned solely in the design assurance aspects of software development.

Acquisition organizations are also interested in quality software; however, they must also consider managerial issues such as cost and schedule. To mitigate known risks many organizations require their suppliers to be SW-CMM assessed to a specific level.

Because avionics developers are striving for design assurance, certification, and efficient processes, many are applying both SW-CMM and DO-178B/ED-12B. This has led to the question: “Can SW-CMM be used as a substitute for DO-178B/ED-12B?” (i.e., can SW-CMM be considered an alternate means of compliance to DO-178B/ED-12B?). While there are many similarities between DO-178B/ED-12B and SW-CMM, there are also a number of significant differences that make it clear that SW-CMM is not an acceptable alternate means of compliance to DO-178B/ED-12B—especially for the more safety critical systems. Even when SW-CMM is used on a project, the objectives of DO-178B/ED-12B must be met for the specific software level.

Together SW-CMM and DO-178B/ED-12B create a quality software process. Companies that have SW-CMM level 2 or higher are more able to apply DO-178B/ED-12B efficiently and across product lines. Some software experts believe that it requires at least a level 2 or 3 maturity in order to apply DO-178B/ED-12B effectively; i.e., DO-178B/ED-12B is intended for mature organizational use. This has led to some difficulties in applying DO-178B/ED-12B, as most software development organizations are level 1. Aviation manufacturers can benefit by the combined use of SW-CMM and DO-178B/ED-12B for certification projects. Unfortunately, many companies use excessive resources by trying to apply DO-178B/ED-12B and SW-CMM separately, to the exclusion of one or the other. The best approach is to integrate the SW-CMM and DO-178B/ED-12B processes.

Many companies have a difficult time integrating the SW-CMM and DO-178B/ED-12B processes successfully. Below are a few items that should be carefully considered when

striving to integrate. The items are not in any particular order.

1. Evaluate current processes.

If the company already has software processes in place, it is beneficial to examine those processes in order to determine if change is needed. Some things to consider are:

- Do the current processes meet DO-178B/ED-12B objectives for the appropriate level?
- Has the process in place been evaluated on a project by the FAA?
- Are the current processes consistent across projects and product lines?
- Has the company performed an internal SW-CMM assessment?
- Have the processes been evaluated by an independent SW-CMM evaluator/assessor?
- Do the current processes meet the desired SW-CMM level?

If the answer is "no" to any or all of these questions, there will likely need to be some revamping of the company processes. In most cases, the change in processes will simultaneously benefit the company's ability to meet SW-CMM and DO-178B/ED-12B.

2. Perform a mapping between DO-178B/ED-12B and SW-CMM.

It is nearly impossible to perform a general comparison between the DO-178B/ED-12B and SW-CMM compliance, because both are designed to be flexible for company implementation. Therefore, the comparison should be done by the company for the particular implementation. It is beneficial to perform a mapping. Starting with either DO-178B/ED-12B or the SW-CMM, map the existing company processes against the selected assurance standard. This will result in a list of evidences to support a claim as meeting either a key process area from the SW-CMM or an objective from DO-178B/ED-12B, depending on the starting point. The remaining assurance standard can then be mapped to expose any remaining deficiencies. The mapping should be performed by a team of company experts; it might even be beneficial to bring in external experts. The team should include experts in SW-CMM, DO-178B/ED-12B, each product line, current company processes, and other areas as needed.

The FAA recently performed a mapping between the FAA-iCMM and DO-178B/ED-12B to determine the compatibility of the two assurance documents for acquiring ground systems. FAA-iCMM combines SEI's SW-CMM, SA-CMM, and SE-CMM; therefore, the scope is slightly different than a strict SW-CMM to DO-178B/ED-12B comparison. However, the trends that were discovered in this mapping are applicable to those who apply SW-CMM as well.

The DO-178B/ED-12B to FAA-iCMM was performed by a team of DO-178B/ED-12B experts and FAA-iCMM experts. Since the FAA's Research and Acquisition organization is already applying FAA-iCMM to projects, the effort was a one-way mapping to determine what additional effort would be required to implement DO-178B/ED-12B on the FAA projects. The mapping occurred by listing the DO-178B/ED-12B objectives in one column and listing the differences in the second column. Below are some of the major differences between DO-178B/ED-12B and FAA-iCMM discovered during the mapping are listed:

- DO-178B/ED-12B is more specific in what is required for planning.
- DO-178B/ED-12B is more specific in what standards are required.
- DO-178B/ED-12B specifies "object code" in a number of cases—this is not so for FAA-iCMM.
- DO-178B/ED-12B requires integration on the target computer; FAA-iCMM does not specify target computer.
- Partitioning and protection have different connotations between DO-178B/ED-12B and FAA-iCMM. FAA-iCMM has a more traditional meaning—DO-178B/ED-12B focuses on safety partitioning and protection.

- FAA-iCMM does not specifically mention normal and robustness testing for each specific software requirement.
- Statement coverage, decision coverage, and modified condition/decision coverage are not specifically called out in FAA-iCMM.
- FAA-iCMM does not address the certification liaison process or certification specific documents.
- DO-178B/ED-12B control categories are not addressed in FAA-iCMM.
- FAA-iCMM does not address the exercise of archived data.
- FAA-iCMM does not address the protection against unauthorized changes.
- Transition criteria is not explicitly mentioned in FAA-iCMM.

In general, DO-178B/ED-12B is targeted more at the software for a specific product being used in safety-related airborne applications. Whereas the FAA-iCMM was written for all types of systems and deals more at an organization and management level.

The above listing of DO-178B/ED-12B to FAA-iCMM differences is not extensive and only provides an example of the types of things to be considered when performing a company-specific mapping. In almost all cases, the requirements of the two assurance standards are not contradictory but are complimentary. Generally, the mapping results in only minor changes or extensions to already existing company processes.

3. Seek certification authority input.

If a company is establishing new processes, it is advisable to get FAA input as early in the process as possible to ensure that any interpretations of DO-178B/ED-12B are in accordance with any regulatory guidance. This becomes more important as new technology and non-traditional methods are employed. Too often certification authorities are not consulted until the process is already implemented. It is much easier to change a process during the planning stages than after it has been implemented.

Both FAA and industry are striving to have early communication on processes and projects that affect certification outcomes. The early partnering of FAA and industry help to avoid surprises and high risk changes late in the program.

4. Strive for consistency across product lines.

Many companies have excellent processes in one product line, such as the flight controls; however, the processes for other product lines, such as displays, are weak and chaotic. The inconsistency of applying DO-178B/ED-12B across product lines has been a great concern for the FAA. SW-CMM promotes the cross-product line consistency.

When implementing new company-wide processes, representatives from all product lines should be involved. The benefit is the easy transition of personnel from one product line to another.

5. Seek outside help, as needed.

Establishing new processes is a tremendous investment. Unfortunately, it is often difficult for company representatives to see their own processes objectively. In many cases, it is beneficial to seek the help of an independent consultant to provide an objective perspective. Independent consultants also tend to have experience with a number of companies and have seen what does and does not work.

6. Strive to maintain and improve processes.

Once a good process is established, it is essential to strive for maintenance and improvement of that process. As people change jobs and new technologies are introduced, it is easy to slip back into bad habits or processes.

When the processes are set up, there should be a process in place for continuous improvement and for addressing problems as they arise.

Benefits of Using SW-CMM on Certification Projects

There are several benefits of applying the SW-CMM to certification projects already requiring DO-178B/ED-12B. The major benefits are described below:

Cost Benefits

DO-178B/ED-12B does not consider whether a process is efficient; it is only interested in whether it meets the objectives. Issues such as training, management, metrics, and improvement strategies that are found in SW-CMM help predict and reduce the cost of a particular DO-178B/ED-12B development. For example, in many certification projects, the test aircraft is used as a test bed for software debugging. This is not the most cost-effective approach. In an organization with well-defined processes, the software bugs are likely to be addressed prior to installation on the aircraft.

Additionally, SW-CMM encourages developers to learn from previous problems faced, created, and resolved from one project to the next. SW-CMM helps developers increase their long term memory and become less reliant on tribal knowledge. By avoiding repeating the same errors over and over, cost is reduced.

Schedule Benefits

When an aircraft misses its certification date, both the aircraft manufacturer and the responsible avionics developers are penalized for each day the certification is delayed. The lack of management of schedule has led many avionics manufacturers to use high priced consultants and test houses late in the cycle. As expensive as this approach is, it is certainly not as bad as the penalty they would incur if they are the system that holds up certification.

With this in mind, predictability in terms of schedule is essential. The more managed and improved a process is, the more predicable the schedule. SW-CMM promotes predictability.

FAA Confidence

The FAA is currently developing criteria to determine the level of FAA involvement required for software approvals. At the beginning of each project, the FAA will assess both applicant and developer. Assessment criteria will include but not be limited to such things as:

- company history
- company certification experience
- software processes across product lines
- designee support
- company experience with DO-178B/ED-12B

Companies that have higher levels of SW-CMM in place are likely to receive more favorable ratings on the assessment, and hence minimize the level of FAA involvement in the project. This is a significant benefit to both the FAA and industry workloads.

Summary

Higher levels of SW-CMM approval can improve the overall software approval on certification projects. SW-CMM must be considered in conjunction with DO-178B/ED-12B and applied simultaneously. This paper has provided some ideas for successful integration of SW-CMM and DO-178B/ED-12B. Successful application of SW-CMM on certification projects may lead to cost savings, schedule reductions, and higher confidence from the FAA.

References

Paulk, Mark C. Report: “Capability Maturity Model for Software, Version 1.1”, dated February, 1993.

Pressman, Roger S. Software Engineering: A Practitioner’s Approach. McGraw Hill, 1997.

RTCA, document DO-178B/ED-12B, “Software Considerations in Airborne Systems and Equipment Certification”, dated December 1, 1992.